



DEPARTMENT OF THE NAVY

NAVAL SCHOOL OF HEALTH SCIENCES  
BETHESDA, MARYLAND 20889-5611

IN REPLY REFER TO:

NSHSBETHINST 5239.1B

00

DEC 16 1996

NSHSBETHINST 5239.1B

From: Commanding Officer

Subj: NAVAL SCHOOL OF HEALTH SCIENCES (NSHS) INFORMATION SYSTEM  
SECURITY (INFOSEC) PLAN

Ref: (a) SECNAVINST 5239.2  
(b) BUMEDINST 5239.1

Encl: (1) Information System Security Plan

1. Purpose

a. To establish the NSHS INFOSEC Plan (ISSP) and assign responsibilities for its implementation and maintenance.

b. To provide guidance and procedures to ensure that all information systems (IS) and network resources at NSHS are maintained and adequately protected.

2. Cancellation. NSHSINST 5239.1A.

3. Background

a. IS resources are subject to misuse/abuse, fraud, malicious acts, theft, and fire, any of which may result in their loss, damage or destruction.

b. Reference (a) established the Navy IS Security Plan. Reference (b) implements that Plan within the Navy Medical Department. Enclosure (1) complies with DON and BUMED policy on IS security and also serves as the central planning and management tool to ensure the total security environment of all IS and network resources operated under the cognizance of NSHS Bethesda.

4. Objectives. To ensure:

a. Availability of reliable information and automated support required to meet the command's mission by adequately



**DEC 16 1996**

protecting all supported IS and network resources against accidental or intentional destruction, unauthorized disclosure, denial of service, and unauthorized modification.

b. Physical, administrative, procedural, personnel, communications, hardware, software and data element security countermeasures are provided and are adequate to protect against such events as material hazards, fire, misuse, or malicious acts.

5. Scope. The ISSP addresses all elements of any Command IS and network resource to include hardware, software, or data. Printing and imaging equipment or systems that are part of an IS, connected to a network, or driven by a process control or embedded computers are also covered.

6. Policy.

a. Command IS resources are vital resources that facilitate communication and support mission accomplishment. All IS and network resources must be protected by a cost-effective security program that emphasizes continuous employment of appropriate protective measures.

b. Each staff member will adhere to all the requirements of this ISSP and report violations to the Information Systems Security Officer (ISSO).

c. Implementation of this ISSP requires active participation by all staff personnel in the continual security maintenance of all Command IS assets.

d. Individuals not complying with these instructions and found in violation of these regulations will be subject to disciplinary actions.

e. End users are an integral part of the security program and the use of systems and networks in achieving job performance is a privilege that can be revoked.

f. All NSHS IS and network resources must be accredited and have the authority to operate. This accreditation must be updated and approved every three years by the Commanding Officer.



g. In accordance with reference (a), administrative, technical, and physical safeguards must be established to ensure the security and confidentiality of data records and to protect data bases against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual when such information is mentioned.

7. Responsibilities. BUMED conducts site inspections of the NSHS Echelon III ISSP to ensure continued compliance with appropriate IS security requirements. Enclosure (1) identifies responsibilities within the command.

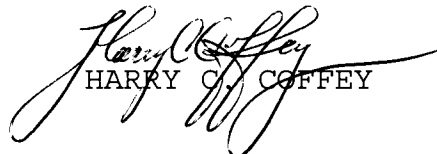
8. Applicability. This ISSP applies to all personnel attached to this Command as well as other personnel who are authorized access to Command systems.

9. Plan Evaluation

a. A comprehensive review of compliance with the ISSP will be conducted as part of the Command Evaluation Program on a biennial basis or when the command's security posture changes. In addition, at any time the Commanding Officer may direct the ISSO to assess compliance with specific elements of the Plan.

b. Specific ISSP functional areas will also be evaluated as part of the Management Control Review (MCR) Program.

10. Action. All personnel using NSHS IS equipment, systems, and data or communicating with such equipment/systems must comply with the regulations contained, or referred to, in enclosure (1).

  
HARRY C. COFFEY

Distribution:  
List I and II

Copy to:  
NAVMEDINFMGMTCEN (Code 13)



# **INFORMATION SYSTEMS**

## **SECURITY PLAN**

NAVAL SCHOOL OF HEALTH SCIENCES

8901 Wisconsin Ave

Bethesda, Maryland

20889-5611

UIC: 0622A

ENCL [ / ]



TABLE OF CONTENTS ..... i

1. PURPOSE ..... 1

2. SCOPE ..... 1

3. ASSUMPTIONS ..... 1

4. ORGANIZATION AND RESPONSIBILITIES ..... 2

5. AIS CONFIGURATION DESCRIPTION ..... 7

6. AIS SECURITY TRAINING ..... 8

7. LIFE CYCLE MANAGEMENT (LCM)..... 9

8. HARDWARE ..... 10

9. SOFTWARE ..... 11

10. DATA..... 11

11. ENVIRONMENTAL SECURITY ..... 12

12. USER ACCESS..... 12

13. NETWORK..... 13

14. VIRUS PROTECTION ..... 13

15. SECURITY THREAT/VIRUS INCIDENT REPORTING ..... 14

16. ACCREDITATION PLAN ..... 15

APPENDIX A - REFERENCES ..... A-1

APPENDIX B - DEFINITIONS & ACRONYMS ..... B-1

DEFINITIONS ..... B-1

ACRONYMS..... B-39

APPENDIX C - IS ORGANIZATION CHART ..... C-1

APPENDIX D - FORMAT TO REPORT SECURITY THREAT/VIRUS INCIDENT ..... D-1

APPENDIX E - SAMPLE ASDP ..... E1



APPENDIX F - REQUEST USE OF PERSONAL AIS RESOURCES.....F-1

APPENDIX G - REQUEST FOR LOAN OF PERSONAL PROPERTY..... G-2



1. **Purpose.** Department of the Navy activities are required to implement a cost effective Information Systems Security (INFOSEC) Plan to protect all organizational assets. To protect the Information System (IS) resources at this command, each IS and network must be accredited as secure. This INFOSEC Plan (ISSP) is a composite of guidance contained in Appendix A references and governs the IS operating environment of NSHS. Appendix B is a listing of common IS definitions and acronyms. The ISSP defines policy and establishes guidance to insure availability of dependable IS resources used in support of the command's mission. This plan is designed to:

- a. Provide information and guidance to all command personnel on measures to protect command IS hardware, software, networks, and data stored therein.
- b. Document the current INFOSEC environment, establish individual responsibility and accountability, delineate specific actions that support the Command ISSP.
- c. Insure IS security accreditation.

## 2. **Scope**

- a. This Plan is the central planning and management tool to establish and maintain the command's INFOSEC environment.
- b. This ISSP includes all security elements that contribute to the protection of all IS resources used in support of the command's mission. The following elements of security are involved in the ISSP: hardware, software, physical/facility security, personnel, communications, and data. These elements provide an environment in which IS resources will operate and maintain security. IS resources include networks, standalone facsimile (FAX) machines, personal computer systems, and all associated peripheral equipment, such as printers, plotters, disk drives, video displays, modems or other communications devices.
- c. This ISSP applies to all military, civilian, and other personnel who are authorized access to Command IS resources or data.

## 3. **Assumptions**

- a. The ISSP is a live working document; it must be continuously revised and updated due to the dynamics of information systems technology and the evolving NSHS Bethesda mission.
- b. Technical support and assistance will be available from Navy Medical Information Management Command (NMIMC) to insure that staff members appointed as Security Officers are capable of meeting their responsibilities under this Plan.



c. Higher authority in the chain of command will actively support IS security measures and will provide necessary resources.

d. The awareness, involvement, and support of all NSHS Bethesda staff are essential to the successful execution of this Plan.

4. **Organization and Responsibilities.** The organization of the IS security staff is displayed in Appendix C. Specific responsibilities of each level include:

a. Commanding Officer (CO):

(1) Act as the Designated Approving Authority (DAA) to:

(a) Decide that an IS or network may operate based on an acceptable level of risk considering the operational need for, and threats to, the system.

(b) Issue an accreditation statement that certifies those IS resources that adhere to appropriate certification and risk management process.

(c) Authorize operation of non-accredited IS resources by issuing an Interim Authority To Operate (IATO) for a period not to exceed one year.

(d) Issue accreditation or IATO for an entire system or group of systems in those instances where such "blanket" IATO or accreditation represents the most efficient means of maintaining system operability while ensuring security.

(e) Review accreditation every three years or when changes to the functionality, architecture, data processed, user population, or environment may result in increased exposure of the IS, network, or computer resource to harm. If no such change has taken place, the accreditation may be reissued based upon a thorough review of the previous accreditation documentation.

(2) Monitor the performance of the Information Systems Security Manager (ISSM) and other IS security staff members.

(3) Fund actions necessary to comply with this Plan.

(4) Prescribe security requirements and standards.

(5) Appoint, in writing, an ISSM and all necessary Information System Security Officers (ISSO), Network Security Officers (NSO), and forward copies of appointing letters to NMIMC and MED-09D.



(6) Establish the operational value of all IS assets and specify necessary operational controls.

b. Command Information Systems Security Manager (ISSM). The position is a full-time function and reports directly to the CO concerning all IS security matters. The ISSM shall have a solid background in computer basics and knowledge of the DON AIS security program. The following duties and responsibilities apply to the ISSM position:

(1) Advise the Commanding Officer on all IS security matters and act as the command coordinator for all IS security matters.

(2) Implement and maintain the NSHS Bethesda ISSP.

(3) Conduct inspections of all command elements to ensure continued compliance with this Plan to maintain accreditation and approval to operate.

(4) Evaluate security procedures to ensure their continued effectiveness.

(5) Provide guidance, advice, and assistance to the Directorates.

(6) Ensure the IS Security and Training Program addresses all elements of the command.

(7) Develop budget input for and execute actions necessary to comply with this Plan.

(8) Investigate all security incidents and submit required reports to higher authority.

(9) Coordinate the Command Risk Assessment program.

(10) Ensure that risk assessments are conducted and implement safeguards to eliminate or minimize identified threats and vulnerabilities. Risk assessments are required every three years or upon any significant change to processed data sensitivity levels, operating system, or network software change.

(11) Provide guidance and training to the ISSOs in the management of system access controls, backup procedures, virus protection and password management.

(12) Ensure all copyright laws for microcomputer software are followed with the assistance of the Directorate ISSOs.

(13) Assume the duties of any IS staff member not appointed or unable to perform their duties.



(14) Develop and maintain contingency plans for mission critical systems and networks.

(15) Classify all IS assets and specify protection controls commensurate with their value.

(16) Authorize access and assign custody of equipment and data to appropriate personnel.

(17) Communicate control and protection requirements to custodians and users.

(18) Monitor compliance and periodically review control and classification decisions.

(19) Ensure position descriptions for personnel assigned IS security responsibilities and duties are accurate and up-to date.

c. Directors. Responsible for all resources under their control, they perform the following duties and responsibilities:

(1) Provide and maintain a complete, accurate inventory of IS equipment and proprietary software.

(2) Assist the ISSM in implementing and maintaining the command's ISSP for all IS resources and networks under their cognizance.

(3) Notify in writing the Administrative Directorate of all nominees for ISSO. Administration Support Department will prepare the appointing letters and forward copies to the ISSO's, NMIMC and MED-09D.

d. Network Security Officer (NSO). The NSO will:

(1) Ensure that countermeasures and security requirements are implemented for each node of the network.

(2) Develop and promulgate the standard security procedures governing network operations.

(3) Ensure that security measures and procedures used at network nodes fully support the security integrity of the network.

(4) Maintain liaison with all Information System Security Officers in the network.



e. Information System Security Officer (ISSO). The duties of the ISSO are similar to the duties of the ISSM, but for specific assigned areas. The ISSOs report to the ISSM. Duties include:

(1) Coordinate system security matters with the ISSM.

(2) Be the focal point for all Directorate IS security matters.

(3) Assist in implementing the ISSP.

(4) Maintain an inventory of all IS hardware, implemented system software packages, and major functional application systems (i.e., finance, personnel, logistics, etc.). Report every resource movement or change to the Command ISSM and Property Manager.

(5) Monitor system activity, including identification of the levels and types of data handled by the IS and networks and verify assignment of passwords for every system assigned to that Directorate.

(6) Assist MIS staff in the installation, upgrade, maintenance, and troubleshooting of Directorate IS equipment. The ISSO is the first point of contact for end user assistance.

(7) Prepare and submit a report on any security threat or virus incident, see paragraph 15 for details and Appendix D for report format.

f. End Users. Security related tasks associated with the use of computer systems rests with each individual end user. Users are responsible to avoid fraud, waste, and abuse of IS resources. Additional responsibilities include, but are not limited to the following:

(1) The most important user responsibility is the protection of passwords from intruders.

(2) Support and promote good security practices.

(3) Follow the established procedures of the NSHS IS Security Program.

(4) Comply with the command's software copyright policy and never use unapproved software.

(5) Log off when leaving the computer area.



(6) Do not remove government owned IS resources (hardware, software, data, other computer devices, etc.) from the command's premises without proper pass control documentation.

(7) Do not process classified in the computer unless proper clearance has been granted by the DAA.

(8) Make backup copies of all critical data files.

(9) Notify your designated ISSO of any security threat or virus incident, see paragraph 15 for definition of incidents.

g. Security Manager (SM). A Security Manager has been appointed to manage the NSHS Information and Personnel Security Program. The Security Manager's responsibilities include but are not limited to the following:

(1) Serve as the command advisor and representative on security of classified information.

(2) Develop written command information and personnel security procedures.

(3) Formulate and coordinate the Command Information Security Education program.

(4) Ensure threats to security (i.e., compromises and other security violations) are reported, recorded, and investigated.

(5) Ensure personnel security investigations, clearances, and accesses are recorded.

(6) Ensure continuous evaluation of personnel security, policies, and procedures.

(7) Establish security control of visits.

h. Privacy Act Coordinator (PAC). The Privacy Act Coordinator is responsible for implementing Privacy Act requirements within the command and performs the following functions:

(1) Serves as the principal point of contact on all Privacy Act matters.

(2) Coordinates Privacy Act requirements with other members of the security staff.



(3) Provides training in the provisions of Privacy Act of 1974 to activity personnel.

(4) Ensures adequate safeguards are enforced to prevent misuse, unauthorized disclosure, alteration or destruction of personal information records.

i. Security Officer (SO). The Security Officer manages NSHS's Physical Security and Loss Prevention Program. The Security Officer's responsibilities include, but are not limited to the following:

(1) Establish, maintain, and administer an ongoing employee physical security and loss prevention education awareness program.

(2) Establish personnel identification and access control systems.

(3) Manage physical security surveys, inspections, and command evaluations.

(4) Coordinate technical assistance effort between IS Security Staff members and end users to provide expertise in all physical security matters.

5. **IS Configuration Description.** All IS resources will be controlled, managed and installed by the ISSM, or a designated representative.

a. Hardware

(1) Microcomputers used at NSHS are Commercial-off-the-shelf (COTS) hardware.

(2) The Command IS inventory processes only unclassified and sensitive unclassified information. The various hardware peripherals used at this command include:

(a) PC and Macintosh architecture used in either a "standalone" or networked mode.

(b) Network server systems.

(c) Portable computers.

(d) Scanners.

(e) Laser, Dot Matrix, Bubble Jet, and High Speed Printers.

(f) Standalone Facsimile (FAX) machines.



(g) Modems.

b. Software. The software packages utilized at the command are COTS programs, security software provided by NMIMC, programming software used in developing and generating programs used for database applications, and as training tools in an "interactive" teaching environment.

c. LAN Network System. The NSO is responsible for the installation of all personal and shared accounts on the network. The LAN server supports two distinct operating environments, that are outlined as follows:

(1) The DOS, Microsoft Windows and New Technology (NT) environment to promote:

(a) access to shared software resources which encourage users to share files and information, thus, reducing "Hard Copy" paperwork.

(b) utilization of additional disk space and printer resources.

(2) The UNIX/Microsoft New Technology Advanced Server (NTAS) environment provides Electronic Mail (E-Mail) capability and fosters IS security controls implemented on the server as follows:

(a) password access.

(b) audit trail of unauthorized access attempts.

(c) file restrictions for unauthorized individuals.

(d) E-Mail provides a paperless communication asset.

## 6. IS Security Training

a. A Security Training and Awareness Program will be in place to provide training for the security needs of personnel accessing an IS or network resource. The Program shall ensure that all personnel responsible for an IS or network resource, and/or the information contained therein and all persons who must access them are aware of proper operational and security procedures and risks.

b. Training on security updates will be provided via regularly scheduled Command General Military Training and as necessary to ensure compliance with the current DON standards.



c. AIS security training is the responsibility of the ISSM. Each ISSO must receive instruction on IS Security. The training program must follow requirements of reference (c). Specifically, the NSHS Bethesda AIS Security Training Plan must be:

(1) Developed and maintained by the ISSM.

(2) Presented to all new staff personnel during command orientation.

(3) Recorded in training records.

(4) Conducted during scheduled General Military Training, and other times as required.

d. AIS concepts to be reviewed and discussed include but are not limited to:

(1) Storage of IS hardware and software.

(2) Access authority to IS equipment.

(3) Password security.

(4) Requirements and procedures to backup data files.

(5) Scanning the systems for viruses.

(6) Security of IS equipment and data.

(7) Use of privately owned software or hardware.

(8) Copyright rules for software.

7. **Life Cycle Management (LCM)**. Action shall be taken throughout the life cycle of all IS resources to ensure compliance with security policies.

a. The ISSM/ISSOs must ensure that all necessary security requirements are evaluated and carefully documented in the Abbreviated Systems Decision Paper's (ASDP's) recommended procurement for new hardware and or software. The Information Systems Executive Board (ISEB) ensures that consideration of IS security is addressed in each ASDP. A request to modify an IS must be submitted to the Commanding Officer, via the ISEB, for approval or disapproval and the request must clearly state specific rationale for the need-to-modify. See Appendix E for an example ASDP.



b. The requesting organization, the ISEB, and the Commanding Officer will ensure the early and continuous involvement of all staff personnel in defining future security requirements for all systems assigned.

c. Acquisition and procurement documents for all Directorates of the Command IS resources will comply with reference (c).

d. Computer security will be built into systems such that system users are relieved of the details of assessing, testing and developing security for that system to the maximum extent possible.

## 8. Hardware.

a. Privately Owned Resources. Use of privately owned or leased IS resources to conduct official Department of the Navy business in the command is allowed only with the prior written authorization of the Commanding Officer. See Appendix F for format of request. Privately owned computers shall not be used to process classified data.

b. Equipment Accountability and Removal. Laptop/notebook (portable) computers used by Command personnel outside of the command's environment (i.e., assignments during TAD travel) will be strictly controlled. Loans of accountable equipment will be made only when the following criteria have been met:

(1) The loan is in the interest of the command and not for personal gain.

(2) Property managed by Department maintaining custody of the system will be returned prior to the scheduled date, if requested by the respective Department Head. The loan will normally not be in excess of fourteen (14) days. An extension of this time frame due to specific circumstances must be approved by the Department Head.

(3) Command personnel with custody of IS assets are financially responsible and require the safeguarding of all hardware, software, data, and for preventing unauthorized access to these assets.

(4) All IS assets that are taken out of the building must have a properly completed Property Pass (Optional Form 7) or NAVCOMPTMAN Form NMC085179, or a copy of a loan agreement signed by the Department Head. See Appendix G for a sample Loan Agreement.

c. User Maintenance and Repair. If a computer asset becomes damaged or specific problems arise, the staff member must report this incident to their TASO or ISSO immediately. If the ISSO can solve the problem, then the ISSO will contact the ISSM with all pertinent information. The ISSM will resolve the situation by using all sources available for assistance (i.e., other staff personnel, NMIMC, or outside vendors.)



9. **Software.**

a. All systems must have back-up capabilities, such as tape drives or floppy disk drives to ensure day-to-day operations are maintained. Data files should be backed up on an alternate media source, at least monthly. Data files with daily changes and/or highly critical to our mission should be backed up more frequently (weekly or daily). End users are responsible for ensuring backup copies of all data files within their areas of responsibility are current.

b. Copyrighted software will not be copied or modified beyond the specifications of the copyright holder. NSHS policy requires strict adherence to patent rights requirements and copyright licensing agreements for all software used in the command. All proprietary software media will be physically controlled by the Management Information Systems Department.

c. Privately owned or developed software (includes public domain, freeware, and shareware) will **not** be used on any Command IS without prior written approval of the Commanding Officer. See Appendix F for format of request.

d. Software will only be installed by the Management Information Systems Department, or an ISSO and any changes or modifications of legal software on a command system are prohibited.

e. Transfer of proprietary software from one system to another is not permitted without the approval of the MIS Department Head and when appropriate, approval by the ISEB.

10. **Data**

a. No classified information will be processed on any IS or network without prior written permission from the Commanding Officer.

b. Directors must determine which data files are critical to their mission, furnish a list to the ISSM, and ensure that these files are backed up by the end users or system administrators. These back-up data files will enable the command to fulfill its mission in case of detrimental events. The ISSM is responsible, with the assistance of all the ISSO's, to ensure that:

(1) Directorate backup procedures for designated critical files are completed on a monthly basis by the identified staff personnel.

(2) The back-up files will be collected by the first of each month and given to the ISO for proper off-site storage.



(3) ISSO's will provide training to their Directorate staffs on correct procedures for backing-up data files.

c. The system user is responsible for protection of any confidential or private database and will ensure that unauthorized personnel can not gain access to this information.

#### **11. Environmental Security.**

a. The DAA is responsible for formally granting authority to operate systems based upon an acceptable level of risk. Every precaution should be made to protect all IS and network resources in all areas and be physically protected against water damage, excessive heat and unauthorized access.

b. The command will provide physical security for IS assets consistent with the physical characteristics of the Directorate, its vulnerability within the IS environment, and the level of data being processed. The most efficient and effective measure to enhance physical security is to secure unoccupied offices. This procedure can provide the physical measure necessary to safeguard and prevent unauthorized access to equipment, material, computer media, and information.

c. Whenever possible, IS resources will be operated within the manufacturers' optimum temperature and humidity range specifications.

d. False ceilings that conceal steam and water pipes will be checked regularly and any apparent irregularity should be reported immediately to the Facilities Manager.

**12. User Access.** An IS, network or other computer resource will follow the "least privilege" principle so that each user is granted access to only the information to which the user is entitled.

a. There shall be in place an access control policy for each IS. It shall include features and/or procedures to enforce the access control policy of the information contained within the IS.

b. The identity of each user authorized access to the IS shall be positively established prior to authorizing access.

c. Physical, procedural and/or technical controls must be put in place to ensure that only authorized personnel with the need-to-know are allowed to manipulate data. In the absence of positive grants of access, systems should default to no access (least privilege).



DEC 16 1996

d. Access to IS and network resources will be controlled and monitored to ensure each person having access can be identified and held accountable for their actions.

e. Procedures for screening all individuals to ensure a level of trustworthiness that is commensurate with the duties of the individual will be controlled by the system custodian.

f. All computer resources that process or handle sensitive unclassified information shall implement Class C2 functionality (Controlled Access Protection). This security software is designed for personal computers and protects the hardware, software and stored data from unauthorized access or use. Within the BUMED claimancy, only NMIMC approved security software packages will be used.

### 13. **Network**

a. Remote access to command computers is only permitted with prior approval of the ISSM.

b. Protective measures must be established for any Command Bulletin Board System (BBS) or World Wide Web (WWW) site to deny unauthorized access and use of the BBS/WWW. Each BBS/WWW must have a permanent system operator appointed in writing by the Commanding Officer to manage and administer the system.

(1) The administrator for any BBS/WWW must ensure that each program or file uploaded to the BBS/WWW is legitimate and free of malicious code, such as viruses or trojan horses. Unauthorized copies of commercially available software, including operating systems, cannot be uploaded to any BBS/WWW.

(2) The administrator must ensure that the BBS/WWW exhibits a warning statement before the BBS banner or on the WWW home page which in part states "... unauthorized access to this United States Government system and software is prohibited by Title 18, United States Code, Section 1030, Fraud and related Activity in conjunction with computers."

(3) Passwords must be established and utilized for BBS access and daily transactions.

c. NSHS WWW Home Page. The NSO is responsible for creating and maintaining the NSHS WWW Home Page. Directors must forward their input for the WWW Home Page through the Commanding Officer or designated authority for approval.

### 14. **Virus Protection**



a. It is imperative that all staff members perform a virus check on every disk that is introduced to their systems (e.g. visiting students, disks received in the mail, and other peers) as well as disks provided to others. A copy of the command virus checking program is available through the Directorate ISSO representative who can provide assistance and training upon request, and the command shared directory.

b. The ISSM will scan the command network for viruses on at least a weekly basis.

15. **Security Threat/Virus Incident Reporting.** The term "incident" refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event. Examples of incidents include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data. Other adverse events include water damage from overhead pipes, floods, fires, electrical outages, and excessive heat that causes system crashes. Adverse events such as natural disasters and power-related disruptions are not, however, within the scope of this instruction. The following general categories of adverse events are encompassed:

a. Malicious code attacks. Malicious code attacks include attacks by programs such as viruses, trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can furthermore replicate rapidly, thereby making containment an especially difficult problem.

b. Unauthorized access. Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to unauthorized access to files and directories stored on a system or storage media by obtaining superuser privileges. Unauthorized access could also entail access to network data by planting an unauthorized "sniffer" program or device to capture all packets traversing the network at a particular point.

c. Unauthorized utilization of services. An intruder can access information, plant trojan horse programs, and so forth by misusing a system or network's available services.

d. Disruption of service. Users rely on services provided by their system and the network. Perpetrators and malicious code can disrupt these services in many ways, including erasing a critical program, "mail spamming" (flooding a user account with electronic mail), and altering a system functionality by installing a trojan horse program.

e. Misuse. Misuse occurs when someone uses a computing system for other than official purposes such as when a legitimate user uses a government computer to



store personal tax records, Federal job application software and data, or any personally owned software use for official or personal business.

f. Espionage. Espionage is stealing information to subvert the interests of a corporation or government.

g. Hoaxes. Hoaxes occur when false information about incidents or vulnerabilities is spread. In early 1995, for example, several users with Internet access distributed information about a virus call the Good Times Virus, even though the virus did not exists.

16. **Accreditation Plan**. The formal management authorization for operation of a specific application on an IS or network resource is based on the results of a security certification and risk assessment. It is a formal declaration by the DAA that a system is approved to operate in a particular security environment meeting a prescribed set of security requirements. The DAA will approve accreditation based upon completion of the following:

a. **Risk Assessment-(RA)**. Evaluates system assets and vulnerabilities and establishes an expected loss from certain events based on estimated probabilities of the occurrence of those events. Appropriate quantitative and qualitative methods of risk assessment shall be developed and promulgated to provide decision makers with management tools to aid in securing systems without undue administrative burden. Automation of risk assessment should be used to reduce the burden wherever feasible. Risk assessments shall be conducted:

- (1) Prior to design approval.
- (2) To support accreditation.
- (3) A significant change to the system environment.

b. **Security Test and Evaluation (ST&E)** serves as the formal technical evaluation of security features and other safeguards, made in support of the accreditation process. IS resources shall be subjected to an ST&E to ensure that the environmental and operational security requirements have been met. When feasible, the ST&E shall be conducted by a third party approved by the Commanding Officer.

c. **Contingency Planning**. Contingency plans shall be developed and, to the maximum extent feasible, tested to ensure that they function in a reliable manner and that adequate backup functions are in place to ensure that critical service is maintained. The plans:

- (1) Are necessary for all systems essential to performance of an activity's mission.



(2) Are not complete until tested under realistic operational conditions. The complexity of the contingency plan is dependent upon the complexity of the system and its need for mission performance.

(3) Must address both automated and manual backup systems to provide for the continuation of its mission during abnormal operating conditions.

(4) Will be developed, tested and maintained to ensure continued performance of mission support and mission critical functions.

(5) Must be consistent with disaster recovery and continuity of operations plans. Detail and complexity should be consistent with the value and criticality of the systems.



DEC 1 8 2000

## APPENDIX A REFERENCES

1. DODD TS3600.1 of 21 Dec 92, Information Warfare (NOTAL).
2. P.L. 100-235 of 8 Jan 88, Computer Security Act of 1987.
3. OMB Circular A-130 of 15 Jul 94, Management of Federal Information Resources (NOTAL).
4. NSTISSID No. 500 of 25 Feb 93, Telecommunications and Automated Systems Security Education, Training and Awareness.
5. NSTISSD No. 501 of 16 Nov 92, National Training Program for Information System Security (INFOSEC) Professionals.
6. NSTISSD No. 502 of 5 Feb 93, National Security Telecommunications and Automated Information Security.
7. NSTISSP No. 6 of 8 Apr 94, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems, (NOTAL).
8. DODD 5200.28 of 21 Mar 88, Security Requirements for Automated Information Systems (AISs) (NOTAL).
9. DODD C-5200.5 of 21 Apr 90, Communication Security (COMSEC) (NOTAL).
10. DODD C-5200.19 of 23 Feb 90, Control of Compromising Emanations (NOTAL).
11. DODD 5000.2 of 23 Feb 91, Defense Acquisition Policies and Procedure (NOTAL).
12. CJCSI 6510.01 of 1 Sep 93, Chairman of the Joint Chiefs of Staff Instruction, Joint and Combined Communications Security (NOTAL).
13. NSTISSI 4009 of 5 Jun 92, National Information Systems Security (INFOSEC) Glossary (NOTAL).
14. SECNAVINST 5000.2A of 9 Dec 92, Implementation of Defense Acquisition Management Policies, Procedures, Documentation, and Reports (NOTAL).
15. SECNAVINST 5231.1C of 10 Jul 93, Life Cycle Management Policy and Approval Requirements for Information System Projects.



NSHSBETHINST 5239.1B  
DEC 16 1996

16. SECNAVINST 5200.32A of 3 May 93, Acquisition Management Policies and Procedures for Computer Resources.

17. SECNAVINST 5239.3 of 14 Jul 95, Department of the Navy Information Systems Security (INFOSEC) Program.



## APPENDIX B DEFINITIONS & ACRONYMS

Many of the definitions and acronyms listed in this appendix are not specifically addressed in this instruction, however, they are terms used in relation to security with IS resources.

### Part 1 - Definitions

**ACCESS.** (COMSEC) Capability and opportunity to gain knowledge of or to alter information or material. (IS) Ability and means to communicate with (i.e. input to or receive output from), or otherwise make use of any information, resource, or component in an IS. NOTE: An individual does not have "access" if the proper authority or a physical, technical, or procedural measure prevents them from obtaining knowledge or having an opportunity to alter information, material, resources, or components.

**ACCESS CONTROL.** Process of limiting access to the resources of an IS only to authorized users, programs, processes, or other systems.

**ACCESS CONTROL LIST.** Mechanism implementing discretionary access control in an IS that identifies the users who may access an object and the type of access to the object that a user is permitted.

**ACCOUNTABILITY.** Property that allows auditing of activities on an IS to be traced to persons who may then be held responsible for their actions.

**ADD-ON SECURITY.** Incorporation of new hardware, software, or firmware safeguards in an operational IS.

**ADMINISTRATIVE SECURITY.** The management constraints and supplemental controls established to provide an acceptable level of protection for a system. Synonymous with procedural security.

**AIS SECURITY.** See *INFORMATION SYSTEMS SECURITY*.

**ATTACK.** Act of trying to defeat IS safeguards.

**AUDIT.** Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.



DEC 16 1996

**AUDIT TRAIL.** 1. Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. 2. Provides a mechanism for tracking user activities. NOTE: Audit trail may apply to information in an IS, to message routing in a communications system, or to the transfer of COMSEC material.

**AUTOMATED DATA PROCESSING (ADP).** Data processing in an automated fashion (i.e., on a computer). See (A)IS.

**(AUTOMATED) INFORMATION SYSTEM ((A)IS).** An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

**AUTOMATED INFORMATION SYSTEM SECURITY.** Measures and controls that safeguard or protect a security (A)IS against unauthorized (accidental or intentional) disclosure, modification, or destruction of (A)IS resources and data, and denial of service. (A)IS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and devices; and personnel and communication controls needed to provide an acceptable level of risk for the (A)IS and for the data and information contained in the (A)IS. It includes the totality of security safeguards needed to provide an acceptable protection level for an (A)IS and for data handled by an (A)IS.

**AVAILABILITY.** The goal of ensuring that information and information processing resources both remain readily accessible to their authorized users.

**BACKUP.** Producing a copy of system and/or data files on separate media so that the system can be regenerated to an acceptable data loss level in the event of a crisis.

**BACKUP PLAN.** See *CONTINGENCY PLANS*.

**BREACH.** A failure or hole in a security mechanism or procedure that allows a violation of the system security policy.

**BROWSING.** The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

**BULLETIN BOARD SYSTEM (BBS).** A private telecommunications utility, usually set up to share information by leaving messages, and uploading or downloading public domain or shareware software. With the advent of viruses anyone using a BBS to download software should be very cautious.



**CLASS C2.** A set of criteria for evaluating the security features and level of assurance provided by a product, it does not specify or address how to implement the required security features to support system-specific information protection policies. "Class C2" applies to products ... both commercially-available products and custom-developed software, firmware and hardware products ... and the level of trust associated with their performance.

**CLASSIFICATION.** The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. Executive Order 12356 defines the following levels: Top Secret, Secret, Confidential, Sensitive Unclassified, and Unclassified.

**COMMUNICATIONS SECURITY.** Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.

**COMPARTMENTED SECURITY MODE.** (A) IS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following: (a) Valid security clearance for the most restricted information processed in the system. (b) Formal access approval and signed non-disclosure agreements for that information to which a user is to have access. (c) Valid need-to-know for information to which a user is to have access.

**COMPROMISE.** Disclosure of information or data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

**COMPUTER.** The hardware, software, and firmware components of a system that are capable of performing calculations, manipulations, or storage of data. It usually consists of arithmetic, logical, and control units, and may have input, output, and storage devices.

**COMPUTER ABUSE.** Intentional or reckless misuse, alteration, disruption, or destruction of data processing resources.

**COMPUTER SECURITY.** 1. The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in an IS, as well as measures designed to prevent denial of authorized use of the system. 2. Addresses technical and procedural measures that can protect your computer system.



**COMPUTER SECURITY INCIDENT.** Any event in which a computer system is attacked, intruded into, or threatened with an attack or intrusion.

**CONFIDENTIAL (C).** The designation applied to information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security. Example of "damage" include the comprise of information that indicates strength of ground, air, and naval forces in the U.S. and overseas area; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; and revelation of performance characteristics, test data, design, and production data on munitions of war.

**CONFIDENTIALITY.** 1. Assurance that information is not disclosed to unauthorized entities or processes. 2. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

**CONFIGURATION.** Selection of one set of possible combinations of features for a system.

**CONFIGURATION CONTROL.** Process of controlling modifications to a telecommunications or automated information systems hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

**CONFIGURATION MANAGEMENT.** Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures and test documentation of an automated information system, throughout the development and operational life of a system.

**CONTINGENCY PLAN.** Plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency.

**CONTROL ZONE.** The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude unauthorized entry or compromise.

**CONTROLLED ACCESS PROTECTION.** 1. Log-in procedures, audit of security relevant events, and resource isolation as prescribed for class C2. 2. A term which describes the minimum set of automated controls that should be provided to IS resources (i.e., discretionary access control (DAC)), user identification and authentication (I&A), auditing of security-relevant events, and clearing of memory and storage before reuse.



REF ID: A1000

**COUNTERMEASURE.** Any action, device, procedure, technique or other measure that reduces the vulnerability of an IS.

**DATA.** Information with a specific physical representation.

**DATA SECURITY.** Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

**DEDICATED (SECURITY) MODE.** An IS is operating in the dedicated mode when all of its users possess the proper security clearance and have need-to-know for accessing all data processed and stored by the IS. IS resources containing only unclassified information, as well as those containing both unclassified and classified information, can operate in the dedicated mode. All information is handled at the highest classification processed by the system.

**DENIAL OF SERVICE.** Result of any action or series of actions that prevents any part of a telecommunications or IS from functioning.

**DESIGNATED APPROVING AUTHORITY (DAA).** 1. Official with the authority to formally assume responsibility for operating an IS or network at an acceptable level of risk. 2. Responsible for the following: issuing an accreditation statement that records the decision to accept all security risks and countermeasures; determining the acceptable level of data remanence risk for each system that will be accredited; approving software programs and equipment used for clearing and purging data storage media, and approving procedures for removal of external markings from data storage media. Only those persons having DAA cognizance over a particular system or medium have authority to approve purging or clearing procedures. DAA for NSHS is the Commanding Officer.

**EMANATION SECURITY.** The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from the interception and from an analysis of compromising emanations from systems. See TEMPEST.

**EMBEDDED COMPUTER.** Computer system that is an integral part of a larger system or subsystem that performs or controls a function, either in whole or part.

**EMISSION SECURITY.** Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypt-equipment, IS, and telecommunications systems.

**ENCIPHER.** Convert plain text to equivalent cipher text by means of a cipher.

**ENCODE.** Convert plain text to equivalent cipher text by means of a code.



**ENCRYPT.** Generic term encompassing encipher and encode.

**ENCRYPTION.** Using cryptographic means to render information unintelligible in a manner that allows the information to be decrypted into its original form. The process of transforming plaintext into ciphertext.

**END USER.** A person or organization receiving products or services produced by an IS either by access to the system or by other means.

**ENVIRONMENT.** Procedures, conditions, and objects that affect the development, operation, and maintenance of an IS.

**FILE PROTECTION.** Aggregate of all processes and procedures established in an IS designed to inhibit unauthorized access, contaminations elimination, modification, or destruction of a file or any of its contents.

**FILE SECURITY.** Means by which access to computer files is limited to authorized users only.

**FIREWALL.** Used to control access to or from a protected network. Enforces a network access policy by forcing connections to pass through this system, where they can be examined and evaluated. The system can be a router, personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnets.

**FIRMWARE.** Equipment or devices computer programming instructions necessary to the performance of the device's discrete functions are electrically embedded in equipment or devices in such a manner that they cannot be electrically altered during normal device operations.

**FLAW.** Error of commission, omission, or oversight in an IS that may allow protection mechanisms to be bypassed.

**FOR OFFICIAL USE ONLY (FOUO).** Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552.

**FREEWARE.** copyrighted programs that have been made available without charge for public use. See *PUBLIC DOMAIN SOFTWARE*, and *SHAREWARE*.

**GROUP ACCREDITATION.** Accreditation of a group of systems having a common security policy and similar residual risks.



DEC 16 1996

**HARDWARE.** The electric, electronic, and mechanical equipment used for processing data.

**IDENTIFICATION.** Process that enables recognition of an entity by an IS

**IDENTIFICATION & AUTHENTICATION.** The process that enables an (A)IS to recognize an entity and verify the entity's identity.

**IMPERSONATION.** Synonymous with spoofing.

**INADVERTENT DISCLOSURE.** Accidental exposure of information to a person not authorized access.

**INDIVIDUAL ACCOUNTABILITY.** Ability to associate positively the identity of a user with the time, method, and degree of access to an IS.

**INFERENCE.** Refers to the deduction of information for which a user is not authorized from information to which the user is authorized.

**INFORMATION LABEL.** Piece of information that accurately and completely represents the sensitivity of the data in a subject or object. NOTE: Information labels consist of a security label as well as other required security markings (e.g., codewords, dissemination control markings, and handling caveats), to be used for data information security labeling purposes.

**INFORMATION SECURITY.** The result of any system of policies and procedures for identifying, controlling, and protecting, from unauthorized disclosure, information whose protection is authorized by Executive Order or statute.

**INFORMATION SENSITIVITY.** Sensitivity of unclassified information shall be determined in accordance with applicable information protection policies regarding information sensitivity and requirements for its control. Sensitivity shall also be considered with respect to unauthorized disclosure and/or modification. The effect of data aggregation and inference shall be considered when determining the sensitivity of information. Some elements, when considered separately, may each be of relatively low sensitivity; however, when considered collectively, these same elements become significantly more sensitive to unauthorized disclosure.

**INFORMATION SYSTEM.** Any telecommunications, computer related equipment, interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.



**INFORMATION SYSTEMS SECURITY (INFOSEC).** The protection of IS resources against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. IS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the IS and for the data and information contained in the IS.

**INFORMATION SYSTEM SECURITY MANAGER (ISSM).** Person responsible to the activity's DAA who develops, maintains, and directs the implementation of the INFOSEC program within the activity. The ISSM advises the CO on all INFOSEC matters, including identifying the need for additional INFOSEC staff. Serves as the Command's point of contact for all INFOSEC matters and implements the command's INFOSEC program. Previously the ADP Security Officer (ADPSO).

**INFORMATION SYSTEM SECURITY OFFICER (ISSO).** Person responsible for ensuring that security is provided for and implemented throughout the life cycle of an information resource. Responsible for implementing system specific security policies in the operational environment. ISSO's are typically responsible for single-user computers (e.g., personal computers and workstations), multi-user computers or departmental Local Area Networks (LANs). The ISSO assists the ISSM in implementing the command's INFOSEC program for an assigned system or area of control. Previously the ADP Systems Security Officer (ADPSSO).

**INTERIM APPROVAL.** Temporary authorization granted by a designated approving authority for an IS to process classified information and information governed by 10 U.S.C. Section 2315 or 44 U.S.C. 3502(2) in its operational environment based on preliminary results of a security evaluation of the system.

**INTERIM AUTHORITY TO OPERATE (IATO).** See interim approval.

**INTERNAL SECURITY CONTROLS.** Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to only authorized subjects (persons, programs, or devices).

**INTRUSION.** The act of violating the system security policy.

**LEAST PRIVILEGE.** Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. NOTE: Application of this principle limits the damage that can result from accident, error, or



DEC 16 1996

unauthorized use of an IS.

**LEVEL.** See security level.

**LIMITED-ACCESS.** Synonymous with access control.

**LIST-ORIENTED.** Computer protection in which each protected object has a list of all subjects authorized to access it.

**LOCK AND KEY PROTECTION SYSTEM.** Protection system that involves matching a key or password with a specific access requirement.

**LOOPHOLE.** An error of omission or oversight in software or hardware that permits circumventing the system security policy.

**MALICIOUS LOGIC.** Hardware, software, or firmware that is intentionally included in an IS for unauthorized purpose.

**MANDATORY SECURITY POLICY.** A policy that is based on constraints imposed by a recognized authority for the protection of sensitive information and applied uniformly to all users of a computing system.

**MISSION.** A specific task with which a person, or group of individuals, or organization is entrusted to perform.

**MISSION CRITICALITY.** The property that data, resources, and processes may have, which denotes that the importance of that item to the accomplishment of the mission is sufficient to be considered an enabling/disabling factor.

**MODE OF OPERATION.** Description of the conditions under which an IS operates, based on the sensitivity of data processed and the clearance levels and authorizations of the users. NOTE: Five modes of operation are authorized for an IS processing information and for networks transmitting information. (See compartmented mode, dedicated mode, multilevel mode, partitioned security mode, and system - high mode.)

**MULTI-LEVEL SECURITY (MODE).** 1. Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization. 2. Data on your information system is at two or more classification levels and not all users have the clearance for the highest classification of data. 3. An IS is operating in the multilevel mode when one or more of its users do not possess the proper security clearance for accessing the most sensitive classified data processed and stored by the IS. Data classification labels maintained by the system can be trusted.



DEC 16 1996

**NATIONAL SECURITY INFORMATION.** Information that has been determined, pursuant to Executive Order 12356 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated.

**NEED-TO-KNOW.** Access to, or knowledge or possession of, specific information required to carry out official duties.

**NETWORK.** A communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

**NETWORK CONNECTION.** A network connection is any logical or physical path from one host to another that makes possible the transmission of information from one host to the other. An example is a TCP connection.

**NETWORK SECURITY.** Protection of networks and their services from unauthorized modifications, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects.

**NETWORK SECURITY OFFICER (NSO).** Individual formally appointed by a DAA ensure that the provisions of all applicable, directives are implemented throughout the life cycle of an automated information system network.

**OPERATING ENVIRONMENT.** The combination of hardware, firmware, operating system software, and application software being evaluated for certification. Once certified, the operating environment will become a Trusted Computing Base (TCB).

**OPERATING SYSTEM (O/S).** An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to a user and their programs and play a central role in ensuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks and other "system" related functions. Synonymous with terms such as "Monitor," "Executive," "Control Program" and "Supervisor."

**ORGANIZATIONAL SECURITY POLICY.** Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

**OVERWRITE PROCEDURE.** Process which removes or destroys data recorded on an IS storage medium by writing patterns of data over, or on top of, the data stored on the medium.



DEC 16 1996

**PARTITIONED SECURITY MODE.** IS security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by an IS.

**PASSWORD.** Protected/private character string used to authenticate an identity or to authorize access to data.

**PENETRATION.** Unauthorized act of bypassing the security mechanisms of a cryptographic system or IS.

**PERMISSIONS.** A description of the type of authorized interaction a subject can have with an object. Permissions include: read, write, execute, add, modify, delete.

**PHYSICAL SECURITY.** Action taken to protect installations, personnel, equipment, computer media, documents, etc. from damage, loss, theft, and/or unauthorized access.

**PRIVACY.** (1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information. (2) The right to insist on adequate security of, and to define authorized users of information or systems.

**PROPRIETARY INFORMATION.** Material and information relating to or associates with a company's products, business or activities, including but not limited to: financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked as proprietary information, trade secrets or company confidential information. NOTE: Trade secrets constitute the whole or any portion of phase of any technical information, design process, procedure, formula or improvement that is not generally available to the public, that a company considers company confidential and that could give or gives an advantage over competitors who do not know or use the trade secret.

**PROTOCOL.** Set of rules and formats, semantic and syntactic, that permits entities of exchange information.

**PUBLIC DOMAIN SOFTWARE.** Software not copyrighted that can be freely distributed without obtaining permission from the programmer or paying the programmer a fee.

**PURGE.** Removal of data from an IS, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. NOTE: an IS must be disconnected from any external network before a purge.



DEC 16 1996

**REACCREDITATION.** The official management decision to continue operating a previously accredited system. NOTE: Reaccreditation occurs (1) periodically, regardless of system change (based on policy (e.g., DoD 5200.28 requires a three year reaccreditation cycle)) or (2) if major changes have been made to some aspect of the system that impact security.

**READ.** Fundamental operation in an IS that results only in the flow of information from an object to a subject.

**READ ACCESS.** Permission to read information in an IS.

**RECERTIFICATION.** A reassessment of the technical and nontechnical security features and other safeguards of a system made in support of the reaccreditation process. NOTE: The level of effort for recertification will depend on the nature of changes (if any) made to the system and any potential changes in the risk of operating the system (e.g., changes in the threat environment may affect the residual risk).

**RECOVERY PROCEDURES.** Actions necessary to restore data files of an IS and computational capability after a system failure.

**RELEASE MARKING.** Authorized marking placed on a document by its originator for the purpose of imposing restrictions on dissemination of the document and the information it contains.

**REMANENCE.** Residual information that remains on storage media after erasure, or after use of insufficient purging procedures.

**RESIDUAL RISK.** Portion of risk that remains after security measures have been applied.

**RESOURCE.** Anything used or consumed while performing a function. The categories of resources are: time, information, objects (information containers), or processors (the ability to use information). Specific examples are: CPU time; terminal connect time; amount of directly-addressable memory; disk space; number of I/O requests per minute, etc.

**RISK.** The probability that a particular threat will exploit a particular vulnerability of the system.

**RISK ANALYSIS.** Synonymous with risk assessment.

**RISK ASSESSMENT.** Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities



of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures. Risk analysis is part of risk management, which is used to minimize risk by specifying security measures commensurate with the relative value of the resources to be protected, the vulnerabilities of those resources, and the identified threats against them.

**RISK INDEX.** Difference between the minimum clearance or authorization of IS users and the maximum sensitivity (e.g., classification and categories) of data processed by the system.

**RISK MANAGEMENT.** Process concerned with the identification, measurement, control, and minimization of security risks in information systems. It includes risk analysis, cost benefit analysis, countermeasure implementation, and system review.

**SAFEGUARDING STATEMENT.** Statement affixed to a computer output or printout that states the highest classification being processed at the time the product was produced, and requires control of the product, at that level, until determination of the true classification by an authorized person.

**SECRET (S)** The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security.

**SECURITY.** Establishment and maintenance of protective measures intended to ensure a state of inviolability from hostile acts and influences, design deficiencies, system/component failure/malfunction, or unintentional misuse.

**SECURITY AUDIT.** An examination of data security procedures and measures for the purpose of evaluating their adequacy and compliance with established policy.

**SECURITY CLASSIFICATION.** The sensitivity of the information. See Security Level.

**SECURITY CLEARANCE.** A security level associated with an individual having a recognized requirement to access classified information at that level or below. The security level assigned is based on the results of interviews and background investigations conducted by investigative organizations.

**SECURITY EVALUATION.** An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a



SEP 16 1996

product evaluation, is an evaluation performed on the hardware and software features and assurance of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to specific operational mission and is a major step in the certification and accreditation process.

**SECURITY FEATURES.** The security-relevant functions, mechanisms, and characteristics of (A)IS hardware and software. Security features are a subset of (A)IS security safeguards.

**SECURITY FLAW.** Error of commission or omission in an IS that may allow protection mechanisms to be bypassed.

**SECURITY INSPECTION.** Examination of an IS to determine compliance with security policy, procedures, and practices.

**SECURITY LABEL.** Piece of information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable non-hierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information). (See information label and sensitivity label.)

**SECURITY SAFEGUARDS.** Protective measures and controls that are prescribed to meet the security requirements specified for an IS. NOTE: Safeguards may include security features, as well as management constraints, personnel security, and security of physical structures, areas, and devices. (See accreditation.)

**SECURITY SPECIFICATION.** Detailed description of the safeguards required to protect an IS.

**SECURITY TEST AND EVALUATION (ST&E).** Examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of that system

**SENSITIVE COMPARTMENTED INFORMATION (SCI).** All Intelligence Information and material that requires special controls for restricted handling within compartmented channels and for which compartmentization is established.

**SENSITIVE INFORMATION.** Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria



established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. NOTE: Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L 100 235).

**SENSITIVE UNCLASSIFIED INFORMATION.** See unclassified but sensitive information.

**SENSITIVITY.** Classification level plus caveats and handling restrictions.

**SHAREWARE.** Shareware is a distribution method for copyrighted software programs developed by independent programmers or authors. It is a marketing technique rather than a type of software. Programs acquired through the Shareware method may be freely copied and passed on to others but each user is expected to register with the author and pay a usage fee. The fee may include some or all of the following: printed documentation, the latest version of the program on disk, telephone support, free updates, and commissions, but most importantly a legal license to continue using the software. See *Freeware* and *Public Domain Software*.

**SOFTWARE.** Various programming aids that are frequently supplied by the manufacturers to facilitate the purchaser's efficient operation of the equipment. Such software items include various assemblers, generators, subroutine libraries, compilers, operating systems, and industry application programs.

**STAND-ALONE, SHARED SYSTEM.** A system that is physically and electrically isolated from all other systems, and is intended to be used by more than one person, either simultaneously (e.g., a system with multiple terminals) or serially, with data belonging to one user remaining available to the system while another user is using the system (e.g., a personal computer with nonremovable storage media such as hard disk).

**STAND-ALONE, SINGLE-USER SYSTEM.** A system that is physically and electrically isolated from all other systems, and is intended to be used by one person at a time, with no data belonging to other users remaining in the system (e.g., a personal computer with removable storage media such as a floppy disk).

**STORAGE OBJECT.** Object that supports both read and write accesses to an IS.

**SYSTEM.** A process that may include computer hardware, software, data, procedures, and people, so related as to behave as an interacting or interdependent unity. A system has a particular purpose and operational environment. A system may contain one or more components or products.



**SYSTEM ADMINISTRATOR (SA).** A role responsible for the maintenance of the non-security aspect of a system such as a file system and user account maintenance, performance tuning, device management and applications, tool, and operating system.

**SYSTEM HIGH MODE.** 1. An IS is operating in the system high mode when all of its users possess the proper security clearance, but do not necessarily have a need-to-know for accessing all data processed and stored by the IS. IS resources containing only unclassified information, as well as those containing both unclassified and classified information, can operate in the system high mode. All information is handled at the highest classification processed by the system. 2. IS security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following: a. Valid security clearance for all information within an IS. b. Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs). c. Valid need-to-know for some of the information contained within the IS.

**SYSTEM INTEGRITY.** Quality of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

**SYSTEM LIFE CYCLE.** The duration of time that begins with the identification of a need to place a system into operation; continues through the systems design, development, implementation and operation; and ends with the system's disposal.

**SYSTEM SECURITY.** Measure of security provided by a system, as determined by evaluation of the totality of all system elements and COMSEC measures that support telecommunications and IS protection.

**SYSTEM SECURITY EVALUATION.** Determination of the risk associated with the use of a given system, considering its vulnerabilities and perceived security threat.

**TAMPERING.** Unauthorized modification that alters the proper functioning of a cryptographic or IS security equipment or system in a manner that degrades the security or functionality it provides.

**TELECOMMUNICATIONS.** Preparation, transmission, communication, or related processing information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical or electronic means.

**TEMPEST.** Short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information system equipment.



DEC 16 1996

**THREAT.** Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an information system.

**TIME BOMB.** Logic bomb for which the logic trigger is time.

**TOP SECRET (TS).** The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the U.S. or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communication intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific or technological development vital to national security.

**TRAP DOOR.** Hidden software or hardware mechanism that can be triggered to permit protection mechanisms in an IS to be circumvented.

**TROJAN HORSE.** Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification or destruction of data.

**TRUSTED COMPUTER SYSTEM.** IS that employs sufficient hardware and software assurance measures to allow simultaneous processing of a range of classified or sensitive information.

**TYPE ACCREDITATION.** Official authorization by the DAA to employ a system in a specified environment. NOTE: Type accreditation includes a statement of residual risk, delineates the operating environment, and identifies specific use. It may be performed when multiple copies of a system are to be fielded in similar environments.

**UNAUTHORIZED DISCLOSURE.** The revelation of information to individuals not authorized to receive it.

**UNCLASSIFIED.** Information that has not been determined, pursuant to E.O. 12356 or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified.

**UNCLASSIFIED BUT SENSITIVE INFORMATION.** Any information the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under



DEC 16 1996

criteria established by an Executive Order (OR) or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

**USER.** Person or process accessing an IS by direct connections (e.g., via terminals) or indirect connections. NOTE: "Indirect connection" relates to persons who prepare input data or receive output that is not reviewed for content or classification by a responsible individual.

**USER ID.** Unique symbol or character string that is used by an IS to uniquely identify a specific user.

**VALID PASSWORD.** A personal password that will authenticate the identity of an individual when presented to a password system or an access password that will allow the requested access when presented to a password system.

**VALIDATION.** Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an IS by one or more departments or agencies and their contractors.

**VIRUS.** Self replicating, malicious program segment that attaches itself to an application program or other executable system component.

**VULNERABILITY.** Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.

**WORLD WIDE WEB (WWW or W3).** A tool through which Internet users access other Internet front ends, navigators, information, services, and resources.



## Part 2 - Acronyms

ACL	access control list
ADP	automatic data processing
ADPSO	ADP Security Officer (Old title see ISSM)
ADPSSO	ADP System Security Officer (See ISSO)
AIG	address indicator group
AIS	automated information system
ANSI	American National Standards Institute
AOSS	automated office support systems
APU	auxiliary power unit
ARRANT	Advanced Research Projects Agency Network
ASCII	American standard code for information interchange
ASD	Assistant Secretary of Defense
AUTODIN	Automatic Digital Network
CA	1. controlling authority 2. cryptanalysis 3. COMSEC account 4. command authority
CAP	Controlled Access Protection
CO	Commanding Officer
COMSEC	communications security
DAA	Designated Approving Authority
DAC	discretionary access control
DIA	Defense Intelligence Agency



DEC 16 1996

DOD	Department of Defense
DON	Department of the Navy
DDN	Defense Data Network
DMA	direct memory access
DSN	Defense Switched Network
ELINT	electronic intelligence
ELSEC	electronic security
EMSEC	emission security
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
FTS	Federal Telecommunications Systems
IATO	Interim Authority to Operate
IBAC	identity bases access control
ICU	interface control unit
IDS	intrusion detection system
INFOSEC	information systems security
I/O	Input/Output
IP	internet protocol
IS	information system
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISS	information systems security



ISSM	Information Systems Security Manager
JCS	The Joint Chiefs of Staff
LAN	Local Area Network
LCM	Life Cycle Management
MAC	1. mandatory access control 2. message authentication code
MIPR	military interdepartmental purchase request
MLS	multilevel security
MOA	memorandum of agreement
MOU	memorandum of understanding
NACSEM	National Communications Security Emanations Memorandum
NACSI	National COMSEC Information Instruction
NCS	1. National Communications System 2. National Cryptologic School 3. net control station
NCSC	National Computer Security Center
NETSEC	Network Security
NIST	National Institute of Standards and Technology
NMIMC	Navy Medical Information Management Command
NSD	National Security Directive
NSDD	National Security Decision Directive
NSO	Network Security Officer
NSTISSI	National Security Telecommunications and Information Systems Security Instruction



NSTISSP	National Security Telecommunications and Information Systems Security Policy .
NTCB	network trusted computing base
NTIA	National Telecommunications and Information Administration
NTISSI	National Telecommunications and Information Instruction
OPR	Office of Primary Responsibility
OPSEC	operations security
PC	personal computer
PROM	programmable read-only memory
RAC	repair action
ROM	read-only memory
SAP	1. system acquisition plan 2. special access program
SCI	sensitive compartmented information
SDNS	Secure Data Network System
SI	special intelligence
SIGSEC	signals security
ST&E	security test and evaluation
STU	secure telephone unit
TCB	trusted computing base
TSEC	transmission security
UCMJ	Uniform Code of Military Justice



DEC 16 1996

UIC	Unit Identification Code
WAN	wide area network
WWMCCS	Worldwide Military Command and Control System



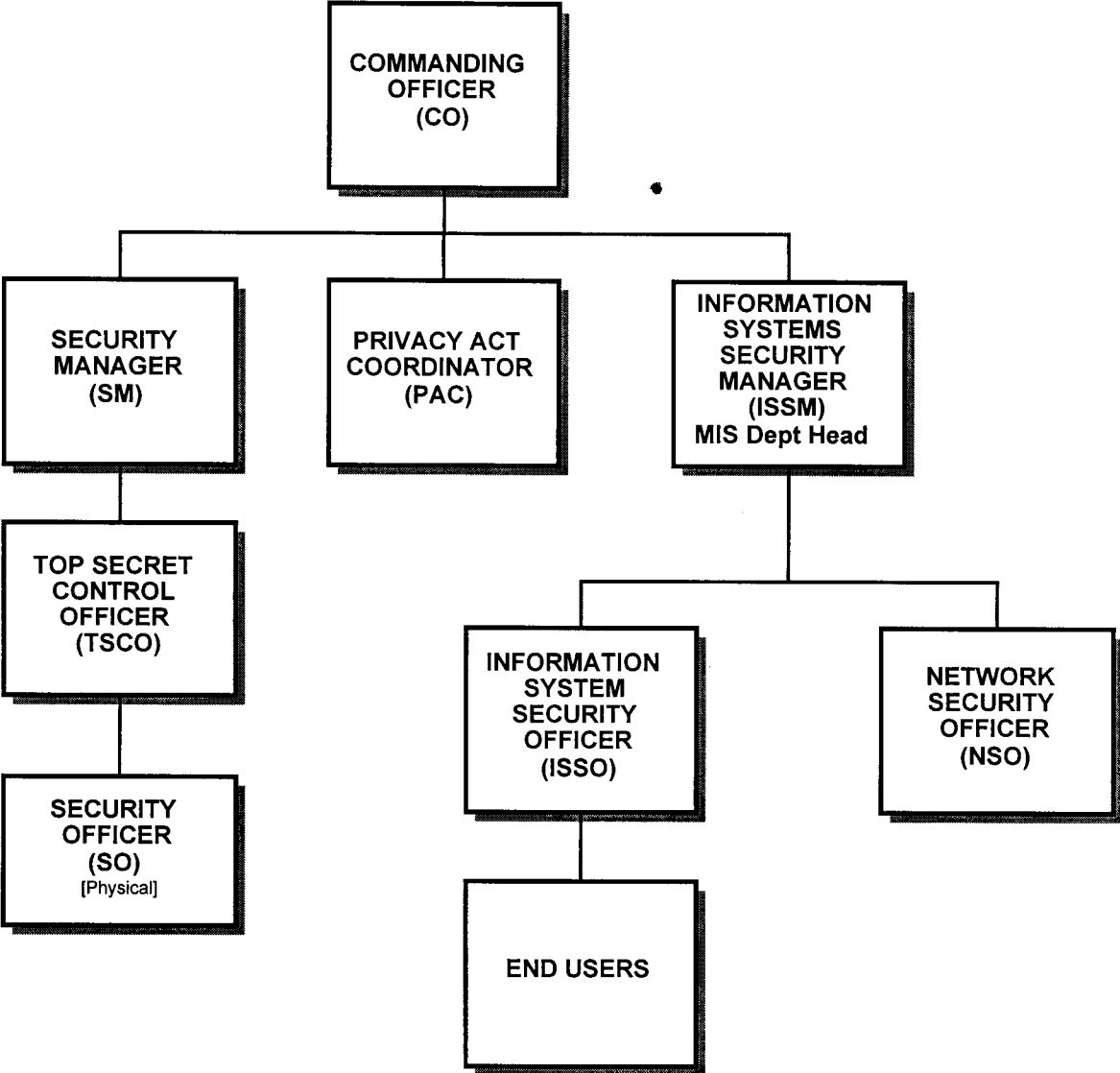
NSHSBETHINST 5239.1B

DEC 16 1996

*Page Intentionally Left Blank*



APPENDIX C  
IS SECURITY ORGANIZATION CHART





NSHSBETHINST 5239.1B

DEC 16 1996

PAGE INTENTIONALLY LEFT BLANK



DEC 16 1996

**APPENDIX D  
FORMAT TO REPORT SECURITY THREAT/VIRUS INCIDENT**

[Date]

**MEMORANDUM**

From: [ISSO Name, Directorate Name]  
To: ISSM, NSHS

Subj: SECURITY THREAT/VIRUS INCIDENT REPORT

Ref: (a) NSHSBETHINST 5239.1B

1. IAW Ref (a), the following security threat/virus incident report is submitted:

- a. Date and time of incident:
- b. System(s) effected:
- c. Location of system(s):
- d. Description of incident: *[For virus infections include: (1) Name of Virus, (2) Source, (3) Other locations outside of NSHS that were possibly infected, and (4) number of diskettes infected.]*
- e. Action taken: *[For virus infections include: (1) Method of clean up, (2) Number of man hours required, and (3) Damage or observations resulting from the virus triggering.]*

\_\_\_\_\_  
Reported By (type/print)

\_\_\_\_\_  
Signature

Copy To:  
Director  
Chairman, Information Systems Advisory Board



NSHSBETHINST 5239.1B

DEC 16 1996

*PAGE INTENTIONALLY LEFT BLANK*



## APPENDIX E SAMPLE ASDP

ASDP# [ASSIGNED BY MIS]

### ABBREVIATED SYSTEM DECISION PAPER (ASDP)

Date Prepared: 28 Mar 96 Major Claimant: BUMED  
Activity and Address: Naval School of Health Sciences  
Bethesda, MD 20889-5612  
Unit Identification Code: 0622A  
Point of Contact: HM1(SS) I. M. Asailor, 295-0845

#### 1. Mission Element Need.

a. The Financial and Materials Management Training Course (FMMTC) is a 12-233k program, providing specialty training to 32 students per year in resource and logistics management. Due to the complex, technical nature of the material taught, computer systems are integral to the curriculum.

b. Currently there are 12 Pentium 100 systems available for the class. The procurement of four (4) additional systems will allow for one computer per student. Computer training is an essential integrated portion of the course requiring a separate PC for each student..

#### 2. Proposed Solution.

a. Procure four additional Pentium 100mhz microcomputer systems in order to have one PC per student.

b. The requirements for the four systems include:

- Pentium based procesor with internal cache
- 32 MB RAM
- 1.2 MB Floppy drive
- 1.44 MB Floppy drive
- 2 GB hard drive
- 32-bit SVGA Card with 2MB
- 17" SVGA color monitor
- 101 enhanced keyboard
- 3 serial, 2 parallel ports
- 1 GB Tape drive

[SAMPLE ASDP Continued]



DEC 16 1996

CD ROM drive  
 Internal FAX modem  
 Multimedia sound kit with speakers  
 Microsoft compatible 3-button mouse and mouse pad  
 Network card (10/100 MB switchable)  
 Surge protector

Standard operating system  
 Standard World Wide Web browser  
 Standard E-Mail  
 Microsoft Office Pro  
 Delrina Form Flow with Fedforms

### 3. Other Alternatives Considered.

- a. Decrease Class size to 12 students.
- b. Procure the systems.

### 4. Costs and Benefits.

COSTS: (\$000)	CY	CY+1	CY+2	CY+3	CY+4	CY+5	CY+6	Total
Hardware	16,000	0	0	0	0	0	0	16,000
Software	8,000	0	0	0	0	0	0	8,000
Installation	0	0	0	0	0	0	0	0
Site Prep	0	0	0	0	0	0	0	0
Maintenance	0	100	100	100	100	100	100	600
Supplies	100	100	100	100	100	100	100	700
Labor	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0
Hardware Upgrade	0	0	500	0	500	0	600	1,600
Communications	100	100	100	100	100	100	100	700
Total	24,200	300	800	300	800	300	900	27,600

Total Acquisition Costs: \$24,200

Total Life Cycle Costs: 27,600

5. Interface Considerations. The systems will interface with the MED-OA and LAN already installed and will be compatible with the current systems.

[SAMPLE ASDP Continued]



DEC 16 1996

- 6. Funding. Command O&M, DHP funds.
- 7. Acquisition Strategy. Upon authorization and receipt of funding, the systems will be ordered in compliance with NSHS and higher directives.
- 8. Other Comments. The FMTC computers will only store or process unclassified data, and they will be physically secured in locked spaces when not in use.
- 9. Specific Approvals. None.
- 10. Joint Signatures.

Requester \_\_\_\_\_

Information System Security Officer \_\_\_\_\_

Comptroller: \_\_\_\_\_

Head, Management Information  
Systems Department \_\_\_\_\_

Modifications: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Technical Approval / Disapproval Recommended:

\_\_\_\_\_  
Chairman, Local Information  
Systems Executive Board

FIP Acquisition Approved / Disapproved :

\_\_\_\_\_  
Commanding Officer



DEC 1 8 1996

**APPENDIX F**  
**FORMAT TO REQUEST USE OF PERSONAL AIS RESOURCES**

**PART I - RESOURCE IDENTIFICATION**

I request use of the following resource:

1. Resource Type: [Software, Hardware, Other]
2. Description:  
[Identify Manufacturer, Model, Serial. Number, Version Number., Etc.]
3. Purpose of Use:  
[Explain why you need to use this resource.]

**PART II - STATEMENT OF UNDERSTANDING**

I have provided proof of ownership by: (Please mark appropriate box with your initials)

Purchase Receipt \_\_\_\_\_ Original Diskettes \_\_\_\_\_

License Agreement \_\_\_\_\_ Other (Explain) \_\_\_\_\_

Permission to use this resource may be withdrawn at any time.

I will use the resource for conducting my official duties and in accordance with the above stated purpose.

The use of this resource will not create a negative impact on command productivity.

All materials or data generated through the at work use of this resource are considered the property of the US Government and will be surrendered should I terminate service with NSHS Bethesda or the US Government.

I will notify my supervisor and the Information Systems Security Officer when use of the resource is no longer needed.

I understand that all US Government instructions, directives, guidelines and procedures apply to this resource while in the confines of NSHS Bethesda. I understand that misuse of the resource (e.g. personal use) may result in disciplinary action.



DEC 16 1996

Name: \_\_\_\_\_ Code: \_\_\_\_\_ Signature: \_\_\_\_\_

Phone: \_\_\_\_\_ Date: \_\_\_\_\_

### PART III - SUPERVISORY/DIRECTORATE APPROVAL

I have reviewed the above request and APPROVE / DISAPPROVE the use of the identified resource.

Estimated Length of Use: \_\_\_\_\_

Reason(s) for Disapproval: \_\_\_\_\_

Additional Remarks: \_\_\_\_\_

Supervisor Name: \_\_\_\_\_ Code \_\_\_\_\_ Signature: \_\_\_\_\_

Phone: \_\_\_\_\_ Date: \_\_\_\_\_

Director Name: \_\_\_\_\_ Signature: \_\_\_\_\_

Phone: \_\_\_\_\_ Date: \_\_\_\_\_

### PART IV - COMMAND APPROVAL (INFORMATION SYSTEMS SECURITY OFFICER)

You are AUTHORIZED / NOT AUTHORIZED use the identified resource.

Beginning Date: \_\_\_\_\_ Expiration Date: \_\_\_\_\_

Review Date: \_\_\_\_\_

[Ending date will not exceed one year. Review date will be 30 days prior to expiration date.]

Remarks: \_\_\_\_\_

ISSM

Name: \_\_\_\_\_ Signature: \_\_\_\_\_

Phone: \_\_\_\_\_ Date: \_\_\_\_\_



DEC 16 1996

**APPENDIX G****REQUEST FOR LOAN OF PERSONAL PROPERTY**

1. **Definition of Loan:** A loan is defined as: "Granting permission to use personal property without compensation on the condition that it will be returned without cost to the Department of the Navy in a condition as good as when loaned, reasonable wear and tear is expected".
  2. **Policy:** Personal property may be lent when legally authorized or when clearly in the interest of the Department of the Navy, NSHS, or national defense. Personal property shall not be utilized for private gain.
  3. **Criteria:** In addition to meeting the basic requirement, loan will meet the following:
    - a. The borrower must be financially responsible.
    - b. Loans will not be in excess of five days without MIS Officer's signature.
    - c. Property will be returned prior to scheduled date, if required by MIS Dept.
    - d. A copy of the approved request will be maintained with the borrowed property at all times.
  4. **Agreement Requirements:** [a-c to be completed by Requestor, d-e to be completed by MIS personnel]
    - a. Borrower's justification for requested loan: \_\_\_\_\_  
\_\_\_\_\_
    - b. Date of loan: \_\_\_\_\_ Date of return: \_\_\_\_\_
    - c. **STATEMENT OF BORROWER:** I, the borrower will assume all liabilities, responsibilities, and costs incurred incident to the loan of this property. I assume all risk of lost or damaged property, and will return the property in as good condition as lent, reasonable wear and tear excepted. System Configuration will not be modified without prior approval of MIS Dept. This agreement and its requirements have been fully explained to me by the approving official.  
  
Name of Borrower: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
Signature: \_\_\_\_\_ Date: \_\_\_\_\_  
Name of Dept Head: \_\_\_\_\_  
Signature of Dept Head: \_\_\_\_\_ Date: \_\_\_\_\_
    - d. Description and condition of property: \_\_\_\_\_  
\_\_\_\_\_
    - e. Serial #/Plant Account #: \_\_\_\_\_
- Approved / Disapproved      MIS Dept Signature: \_\_\_\_\_